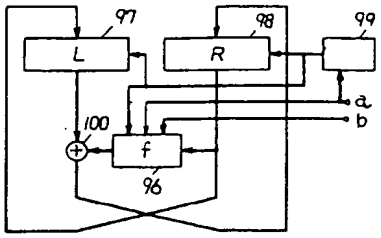
(54) SIGNAL SCRAMBLER AND CIPHERING DEVICE
(11) 5-75596 (A) (43) 26.3.199[illegible]9) JP
(21) Appl. No. 3-230147 (22) 10.9.1991
(71) MATSUSHITA ELECTRIC IND CO LTD (72) NOBORU KATSUTA(3)
(51) Int. Cl⁵. H04L9/06,H04L9/14,G09C1/00

PURPOSE: To obtain a ciphering device for secret communication which is capable of processing of plural ciphering algorithms.

CONSTITUTION: Left and right halves of an input signal are inputted to registers 97 and 98 respectively. A signal scrambler 96 repeatedly scrambles a ciphering key and the output of the register 98 at each time of input of a clock pulse. When a preliminarily set number of clock pulses are inputted, a pulse control circuit 99 sends an update signal to registers 97 and 98 to rewrite contents of registers 97 and 98. This operation is performed as the processing in one stage, and the number of pulses in each stage is independently set.

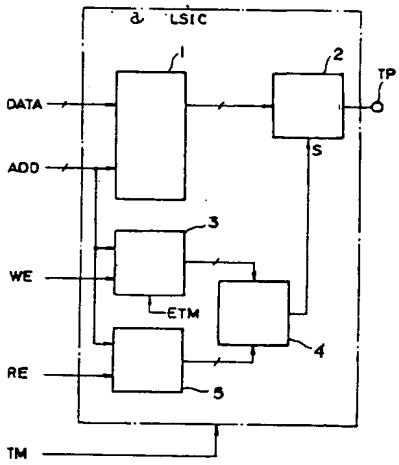


a: clock pulse, b: ciphering key

(54) SECRET KEY PROTECTING SYSTEM AND CIPHER PROCESSING LSIC BY THIS SYSTEM
(11) 5-75597 (A) (43) 26.3.1993 (19) JP
(21) Appl. No. 3-230580 (22) 10.9.1991
(71) FUJITSU LTD (72) HIDEAKI TANAKA
(51) Int. Cl⁵. H04L9/06,H04L9/14,G09C1/00

PURPOSE: To provide the secret key protecting system and the cipher processing of this system where read/write of a memory part where secret key data is stored can be checked but secret key data cannot be observed from the external.

CONSTITUTION: Data in a memory part 1 where secret key information is stored can be read/written from the external in the test mode. A control part 2 which controls permission/inhibition of external output of read data from the memory part 1, a storage part 3 where all stored information are reset by input of a test mode signal TM and information related to addresses where data is written in the memory part 1 is stored thereafter, and a comparing part 4 which compares stored information of the storage part 3 and information related to the address for data read of the memory part 1 with each other are provided. When the test mode is set and the comparison in the comparing part 4 results in coincidence, the control part 2 permits data output. The memory part 1 and a cipher processing part which generates secret key information are unified and integrated into a cipher processing LSIC to improve the secrecy.

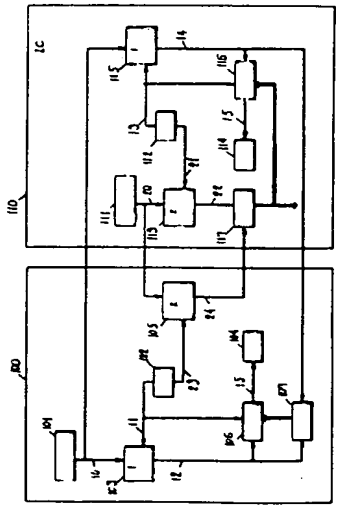


5: gate part, a: cipher processing LSIC

(54) KEY DATA SHARING DEVICE
(11) 5-75598 (A) (43) 26.3.1993 (19) JP
(21) Appl. No. 3-237699 (22) 18.9.1991
(71) MATSUSHITA ELECTRIC IND CO LTD (72) YOSHIHIRO MUTO(1)
(51) Int. Cl⁵. H04L9/06,H04L9/14,G06F12/14,G06K17/00,G09C1/00

PURPOSE: To eliminate a need of decoding processing to share a session key between communicators while confirming it by communicators of each other.

CONSTITUTION: An information processing terminal 100 and an IC card 110 transmit generated random numbers 10 and 20 to each other and cipher the transmitted random numbers to obtain cipher data 12 and 22. Thereafter, they cipher received random numbers of each other to transmit cipher data 24 and 14. They compare received cipher data and data ciphered by themselves with each other; and in the case of coincidence, they use secret key data and operated cipher data to obtain key data common to them by operation.



101,111: random number generating means, 102,112,104,114: memory, 103,115: first cipher means, 105,113: second cipher means, 106,116: processing means, 107,117: collating means

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－75598

(43)公開日　平成５年(1993)３月26日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/06				
	9/14				
Ｇ０６Ｆ	12/14	３２０　Ｃ	9293－5B		
Ｇ０６Ｋ	17/00	Ｔ	8623－5L		
			7117－5K	Ｈ０４Ｌ　9/ 02　Ｚ	

審査請求　未請求　請求項の数４(全　５　頁)　最終頁に続く

(21)出願番号　特願平3－237699

(22)出願日　平成３年(1991)９月18日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　武藤　義弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　高木　伸哉
大阪府門真市大字門真1006番地　松下電器産業株式会社内

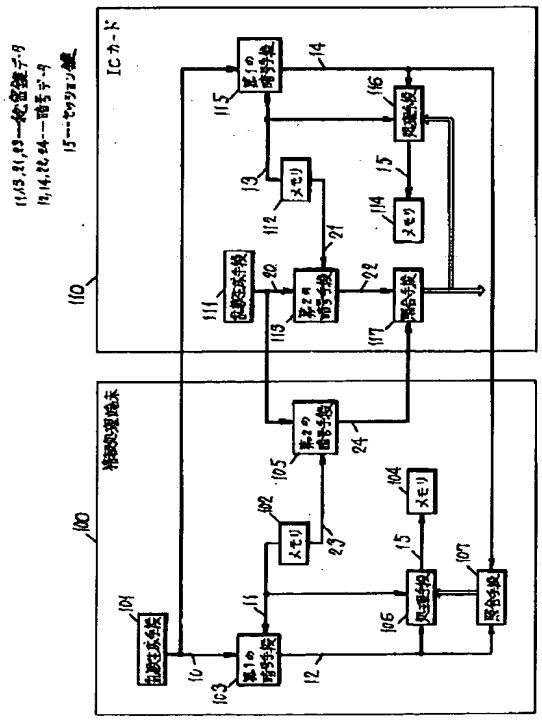
(74)代理人　弁理士　小鍛治　明　(外２名)

(54)【発明の名称】　鍵データ共有装置

(57)【要約】

【目的】　復号処理が不要で、通信者間で相互に認証を行いつつ、セッション鍵を通信者間で共有できる鍵データ共有方式を提供する。

【構成】　情報処理端末１００とＩＣカード１１０はそれぞれお互いに、生成した乱数１０，乱数２０を相手に送信すると同時に、送信した乱数を暗号化して暗号データ１２，暗号データ２２を得る。お互いにその後、それぞれ受信した相手の乱数を暗号化してそのその暗号データ２４，暗号データ１４を送信する。また受信した暗号データと先に自分で暗号したデータを比較し、一致した場合に秘密の鍵データと演算した暗号データとを用いて演算し、お互いの共通鍵データとする。



1

【特許請求の範囲】

【請求項１】乱数を生成する乱数生成手段と、第１の秘密鍵データと第２の秘密鍵データを格納する第１のメモリと、前記第１の秘密鍵データを用いて演算する第１の暗号手段と、前記第２の秘密鍵データを用いて演算する第２の暗号手段と、前記第１の暗号手段によるデータあるいは前記第２の暗号手段によるデータと通信回線から受信したデータとを比較する照合手段と、前記照合手段の結果によって起動し通信したデータと前記第１の秘密鍵データとを用いて演算する処理手段と、前記処理手段の演算結果を格納する第２のメモリより構成される鍵データ共有装置。

【請求項２】ＩＣカードが接続可能な情報処理端末間で行われる鍵データ共有方式であり、前記ＩＣカードは、少なくとも、第１の秘密鍵データと第２の秘密鍵データを格納する第１のメモリと、前記第１の秘密鍵データを用いて演算する第１の暗号手段と、前記第２の秘密鍵データを用いて演算する第２の暗号手段と、前記第１の暗号手段によるデータあるいは前記第２の暗号手段によるデータと通信回線から受信したデータとを比較する照合手段と、前記照合手段の結果によって起動し通信したデータと前記第１の秘密鍵データとを用いて演算する処理手段とを含み、前記情報処理端末は、乱数を生成する乱数生成手段を含み、鍵データ共有方式における演算をＩＣカードが行うことを特徴とする鍵データ共有装置。

【請求項３】乱数を生成する乱数生成手段と、第１の秘密鍵データと第２の秘密鍵データを格納する第１のメモリと、前記第１の秘密鍵データを用いて演算する第１の暗号手段と、前記第２の秘密鍵データを用いて演算する第２の暗号手段と、前記第１の暗号手段によるデータと通信回線から受信したデータとを比較する照合手段とより構成される通信装置。

【請求項４】乱数を生成する第１の手順と、前記第１の手順の後、前記乱数を送信する第２の手順と、前記第１の手順の後、前記乱数を第１の暗号手段で暗号化し第１の暗号データを得る第３の手順と、前記第３の手順の後、受信した暗号と照合する第４の手順と、受信した乱数を第２の暗号手段で暗号化し第２の暗号データを得る第５の手順と、前記第５の手順の後、第２の暗号データを送信する第６の手順よりなる鍵データ共有方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】暗号通信において、通信を行うもの同士が共通の鍵データ（以後セッション鍵と呼ぶ）を共有するための鍵データ共有方式に関する。

【０００２】

【従来の技術】従来、秘密鍵暗号アルゴリズムに基づく暗号処理を実施するために通信者間で使用される鍵は共通の鍵データであり、物理的に安全な方法、たとえば予め装置内に格納して配送するなどの方法で鍵データを共

2

有していた。またこの秘密鍵データは、通信する相手が多数の場合、相当数の鍵データを予め記憶しておく、あるいは通信に参加している人すべてが共通の一つの鍵データを共有している必要がある。暗号通信においてこの秘密鍵が使用された場合、固定データを暗号化しても固定の暗号化データが計算されるので、通信回線上を盗聴されると不正が行われやすく、通常データの暗号化あるいは復号化には直接使用されない。そこで暗号通信には通信毎に変化するセッション鍵を使用する。この秘密鍵データは、セッション鍵を共有するために、鍵データ共有方式で使用される。

【０００３】図２にセッション鍵を共有するための従来の鍵データ共有方式の例を示す。ここで情報処理端末２１０が情報処理端末２２０との間でセッション鍵を共有する方式について説明する。メモリ２１３およびメモリ２２３には、予め共通の秘密鍵データ３１が格納されているものとする。

【０００４】情報処理端末２１０において、鍵データ生成手段２１１は暗号処理を実施するために通信者間で使用されるセッション鍵３０を生成する。メモリ２１３に格納されている秘密鍵データ３１で暗号手段２１２によりセッション鍵３０を暗号化し、情報処理端末２２０に送信する。情報処理端末２２０は受信した暗号データ３２をメモリ２２３に格納されている秘密鍵データ３１で復号化手段２２２により復号化する。復号化して得られたセッション鍵４０は不揮発性のメモリ２２１などに格納して、情報処理端末２１０と情報処理端末２２０との間でデータを共有できる。

【０００５】

【発明が解決しようとする課題】従来の鍵データ共有方式においては、復号手段が必須であり、また暗号通信など暗号処理を行う前に、不正防止のために通信相手の認証処理が必要となる。これら多くの処理はＩＣカードなどの演算能力が低い装置にとってはメモリ容量および処理の負担が大きくなる。

【０００６】本発明はかかる点に鑑み、復号処理が不要で、通信者間で相互に認証を行いつつ、セッション鍵を通信者間で共有できる鍵データ共有方式を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明は上記目的を達成するために、乱数を生成する乱数生成手段、第１の秘密鍵データと第２の秘密鍵データを格納する第１のメモリと、前記第１の秘密鍵データを用いて演算する第１の暗号手段と、前記第２の秘密鍵データを用いて演算する第２の暗号手段と、前記第１の暗号手段によるデータあるいは前記第２の暗号手段によるデータと通信回線から受信したデータとを比較する照合手段と、前記照合手段の結果によって起動し通信したデータと前記第１の秘密鍵データとを用いて演算する処理手段と、前記処理手段の

演算結果を格納する第２のメモリとを含む情報処理端末間により許容される鍵データ共有方式である。

【０００８】

【作用】この方式により許容される鍵データ共有方式は、情報処理端末に格納する秘密の鍵データの数を削減し、また復号処理が不要であるため、メモリ容量および処理を削減することが可能となる。また、相互認証処理を行う都度にランダムな秘密の鍵データを通信者間で共有するため、この共有鍵を使用した安全性の高い暗号化処理が可能となる。

【０００９】

【実施例】以下、本発明の一実施例について図面を参照しながら説明する。図１は本発明の実施例による鍵データ共有方式を示した構成図である。１００は情報処理端末、１１０はＩＣカードであり、情報処理端末１００とＩＣカード１１０との間でセッション鍵を共有する方式について説明する。情報処理端末１００の秘密鍵データ１１と秘密鍵データ２３およびＩＣカード１１０の秘密鍵データ１３と秘密鍵データ２１は予めシステムを管理しているセンターによって格納されるものである。

【００１０】情報処理端末１００は、乱数生成手段１０１により乱数１０を生成し、ＩＣカード１１０に送信する。同時に、第１の暗号手段１０３によりメモリ１０２に格納されている秘密鍵データ１１を用いて乱数１０を暗号化し、暗号データ１２を得る。

【００１１】ＩＣカード１１０は、第１の暗号手段１１５によりメモリ１１２に格納されている秘密鍵データ１３を用いて情報処理端末１００から受信した乱数１０を暗号化し、暗号データ１４を得る。乱数生成手段１１１により乱数２０を生成し、情報処理端末１００に送信する。同時に、第２の暗号手段１１３によりメモリ１１２に格納されている秘密鍵データ２１を用いて乱数２０を暗号化し、暗号データ２２を得る。

【００１２】情報処理端末１００は、第２の暗号手段１０５によりメモリ１０２に格納されている秘密鍵データ２３を用いてＩＣカード１１０から受信した乱数２０を暗号化し、暗号データ２４を得る。その後、暗号データ２４をＩＣカード１１０に送信する。

【００１３】ＩＣカード１１０は、照合手段１１７により暗号データ２２と情報処理端末１００から受信した暗号データ２４を比較する。不一致の場合は、以後の処理は打ち切られ、一致した場合は、暗号データ１４を情報処理端末１００に送信するとともに、処理手段１１６により秘密鍵データ１３と暗号データ１４を用いて演算（例えば排他的論理和）し、この演算結果をセッション鍵としてメモリ１１４に格納する。

【００１４】情報処理端末１００は、照合手段１０７により暗号データ１２とＩＣカード１１０から受信した暗号データ１４を比較する。不一致の場合は、以後の処理＊は打ち切られ、一致した場合は、処理手段１０６により秘密鍵データ１１と暗号データ１２を用いて演算（例えば排他的論理和）し、この演算結果をセッション鍵としてメモリ１０４に格納する。

【００１５】センターによって認められた情報処理端末およびＩＣカードであれば、すなわち、情報処理端末１００の秘密鍵データ１１とＩＣカード１１０の鍵データ１３が同一であり、かつ情報処理端末１００の秘密鍵データ２３とＩＣカード１１０の鍵データ２１が同一であれば、それぞれの情報処理端末あるいはＩＣカードにおける照合手段による結果は一致し、お互いに認証が行え、かつ共通のセッション鍵が共有できる。

【００１６】なお、本実施例では、処理手段１０６および１１６における演算に排他的論理和を用いたが、２つのデータの内一方を鍵データ、他方を平文データとして暗号化することも考えられる。また、この演算に用いられる２つのデータは、秘密鍵データとお互いに同じ演算を施したデータとであればどのような組合せでも可能である。

【００１７】さらに、本発明の鍵データ共有方式によって共有したセッション鍵を用いて、次の暗号処理に用いる鍵データを交換する事も容易である。例えば、共有したセッション鍵を判定パラメータとして、このパラメータと交換したい鍵を用いて、暗号処理を施し相手に送信する。受信者は受信データを復号処理した後、パラメータを判定し、一致すれば次に使用する鍵データを交換する。

【００１８】また、鍵データ共有方式は、高い安全性が要求され、特に情報処理端末１００のメモリ１０２からはデータが読み出せないようにする必要がある。本発明では、ＩＣカード１１０とは別の第２のＩＣカード（以下セキュリティモジュールと呼ぶ）で前記一連の鍵データ共有方式を実施することが可能である。このセキュリティモジュールは情報処理端末に接続した形で使用する。なお、セキュリティ上セッション鍵を格納するメモリは、不揮発性メモリにするのが望ましい。

【００１９】

【発明の効果】以上のように本発明によれば、ＩＣカードに格納する鍵データは２つの秘密鍵だけであり、また処理的にも復号処理は不要となり、メモリ容量は少なくてすむ。また、通信者間で相互に認証を行うため、高い安全性のもとで鍵データの共有が可能である。

【図面の簡単な説明】

【図１】本発明の実施例による鍵データ共有方式を示した構成図

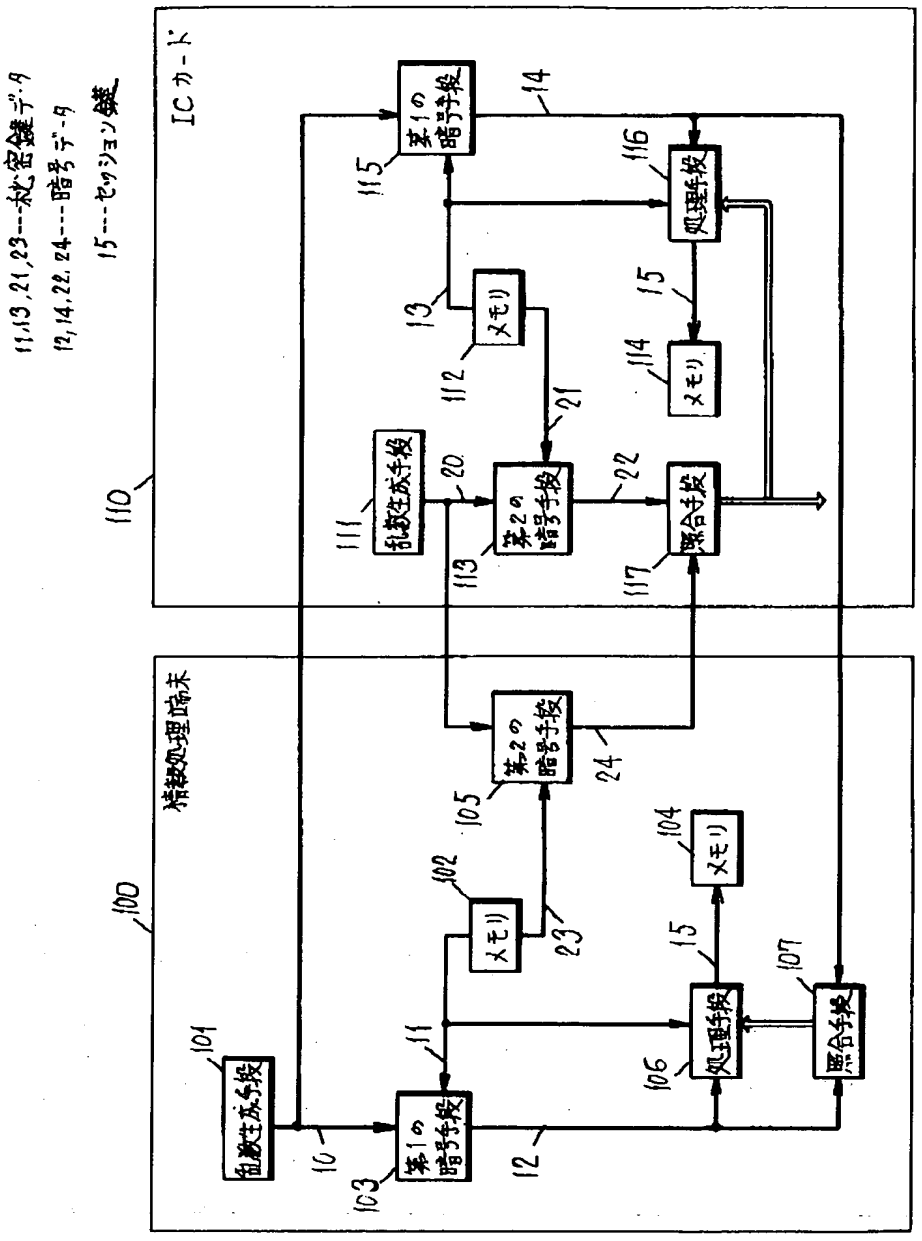
【図２】従来の鍵データ共有方式を示した構成図

【符号の説明】

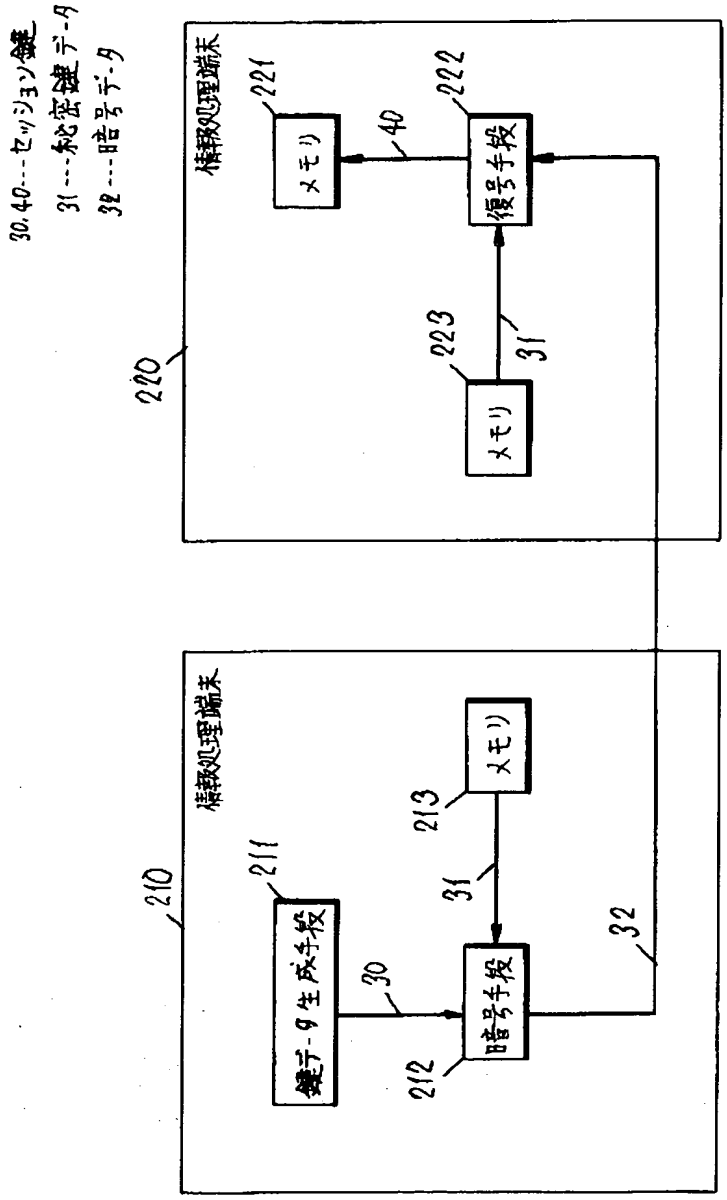
１００　情報処理端末

１１０　ＩＣカード

【図１】


11,13,21,23---秘密鍵データ
12,14,22,24---暗号データ
15---セッション鍵
ICカード
110
乱数生成手段
111
第1の暗号手段
115
メモリ
112
メモリ
114
第2の暗号手段
113
処理手段
116
照合手段
117
情報処理端末
100
乱数生成手段
101
第1の暗号手段
103
メモリ
102
第2の暗号手段
105
メモリ
104
処理手段
106
照合手段
107
10
11
12
15
20
21
22
23
24

【図２】



フロントページの続き

(51) Int. Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０９Ｃ　1/00		9194－5Ｌ		